LANCOM™ VPN Option

Licence Agreement for LANCOM Software Options

User agreement

Enabling of the software option in an LANCOM product is only legally permissible via the downloaded registration key resulting from online registration.

For the online registration and for the receipt of the code, the dedicated licence number acquired legally by purchase of an LANCOM software option my be used only. The licence proof with the imprinted licence number is to be kept carefully.

Reverse engineering or re-assembling is vorbidden.

LANCOM Systems reserves the right to take legal action in case of infringement of any of the afore-mentioned points.

Liability limitations

LANCOM Systems is not liable for any loss or injury resulting from abuse of its products.

SSH® explanantion

LANCOM VPN products are manufactured under license from SSH Communications Security. The following applies for all product components from SSH: © 2002 SSH Communications Security. All rights reserved.

© 2002 LANCOM Systems GmbH, Würselen (Germany). All rights reserved.

While the information in this manual has been compiled with great care, it may not be deemed an assurance of product characteristics. LANCOM Systems shall be liable only to the degree specified in the terms of sale and delivery.

The reproduction and distribution of the documentation and software supplied with this product and the use of its contents is subject to written authorization from LANCOM Systems. We reserve the right to make any alterations that arise as the result of technical development.

Trademarks

Windows®, Windows NT® and Microsoft® are registered trademarks of Microsoft, Corp.

Cisco is a registered trademark of Cisco Systems, Inc.

SSH Secure Shell, SSH IPSEC Express, SSH NAT Traversal, SSH Sentinel and SSH Certifier are trademarks of SSH Communications Security.

The LANCOM Systems logo and the LANCOM brand name are registered trademarks of LANCOM Systems GmbH. All other names mentioned may be trademarks or registered trademarks of their respective owners.

Subject to change without notice. No liability for technical errors or omissions.

LANCOM Systems GmbH
Adenauerstr. 20/B2
52146 Würselen
Germany

www.lancom.de

101481/0802

Preface

EN

Thank you for placing your trust in this LANCOM product.

With *LANCOM VPN Option*, you can enable your *LANCOM* to set up so-called virtual private networks. You can then establish cost-effective network links via the Internet with extremely high data security.

One special feature of *LANCOM VPN* is *Dynamic VPN*, a patent-pending LANCOM Systems technology. While VPNs normally require static IP addresses, *Dynamic VPN* also permits VPN connections using dynamic IP addresses. You can thus use the *LANCOM VPN* with any Internet connection.

This documentation...

... was compiled by several members of our staff from a variety of departments in order to ensure you the best possible support when using your LANCOM product.

In case you find errors or just want to address critics or enhancements, please send an email directly to:

info@lancom.de

Our online services (www.lancom.de) are available to you around the clock should you have any queries regarding the topics discussed in this manual or require any further support. In the Support file section under 'Know-how', you can find answers to frequently asked questions (FAQs). The KnowledgeBase also contains a large pool of information. Current drivers, firmware, tools and manuals can be downloaded at any time.

In addition, LANCOM Support is available. For telephone numbers and contact addresses of the LANCOM Support, please see the enclosed leaflet or the LANCOM website.

Information symbols	
	Very important information. Failure to observe this may result in damage.
	Important information that should be observed.
	Additional information that may be helpful but which is not required.

Special formatting in the body text	
Bold	Menu commands, buttons or input fields
Code	Input and output in command-line mode
<Value>	Placeholder for an actual value
Italics	Notes and product names

Contents

1 Introduction 7
1.1 Package contents of the *LANCOM VPN Option* 7
1.2 What are the advantages of VPN? 7
1.2.1 Private IP addresses on the Internet? 10
1.2.2 Secure communications via the Internet? 10
1.3 VPN connections in detail 12
1.3.1 LAN-LAN coupling 12
1.3.2 Dial-up connections (Remote Access Service) 13
1.4 What is *Dynamic VPN*? 13
1.4.1 A look at IP addressing 14
1.4.2 This is how *Dynamic VPN* works 15
1.5 An overview of *LANCOM VPN* 18
1.6 What now? 19

2 Installation of the VPN option 21
2.1 Installation requirements 21
2.1.1 Package contents 21
2.1.2 Access to the device and *LANconfig* 21
2.1.3 Latest *LANconfig* version 21
2.1.4 Latest firmware version 22
2.2 Online registration 22
2.3 Activating the VPN option 23
2.4 Checking the activation 24

3 Setting up the VPN connection 25
3.1 The *LANconfig* Wizard for VPN 25
3.2 VPN configuration - step-by-step 26
3.2.1 Overview of configuration entries 26
3.2.2 Starting the Assitant 27
3.2.3 General information on the local device and the remote station 29
3.2.4 ISDN connection for Dynamic VPN 30
3.2.5 Passwords for VPN 30
3.2.6 The IP address of the remote station 32
3.2.7 TCP/IP Routing settings 32
3.2.8 NetBIOS routing 35
3.2.9 IPX Routing 35

4 Examples of VPN configurations 39
4.1 Static/static 39
4.2 Dynamic/static 40
4.3 Static/dynamic 41
4.4 Dynamic/dynamic 42

5 The technology behind VPN 43
5.1 How does VPN work? 43
5.1.1 IPSec—the foundation of *LANCOM VPN* 43
5.1.2 Alternatives to IPSec 44
5.2 The standards behind IPSec 46
5.2.1 IPSec modules and their tasks 46
5.2.2 Security associations—numbered tunnels 46
5.2.3 Authentication—the AH protocol 47
5.2.4 Encryption of the packets—the ESP protocol 50
5.2.5 Key management—IKE 52

6 Index 55

EN

1 Introduction

This chapter provides answers to the three following questions:

- What is included in the package contents of the *LANCOM VPN Option*?
- What are the advantages of VPN?
- What are the capabilities and properties of the *LANCOM VPN*?

1.1 Package contents of the *LANCOM VPN Option*

First, please check that the *LANCOM VPN Option* package also contains the following components in addition to this manual:

- Proof of license
- Printed manual
- *LANCOM CD*

1.2 What are the advantages of VPN?

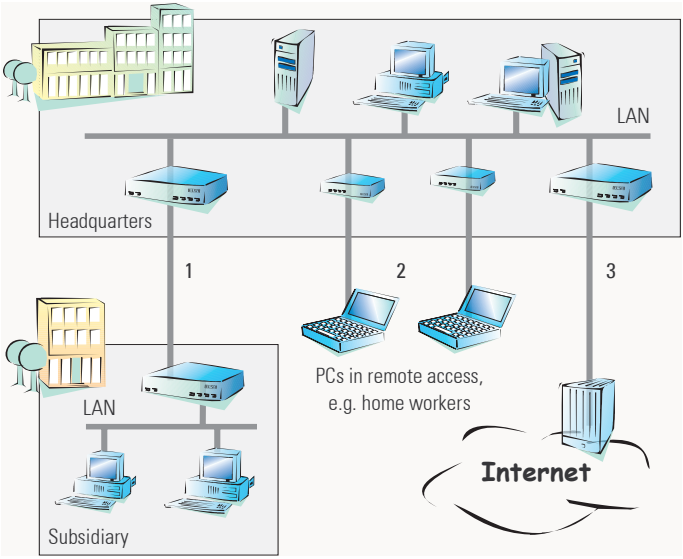
A VPN (**V**irtual **P**rivate **N**etwork) can be used to set up cost-effective, public IP networks, for example via the ultimate network: the Internet.

While this may sound unspectacular at first, in practice it has profound effects. To illustrate this, let's first look at a typical corporate network without VPN technology. In the second step, we will see how this network can be optimized by the deployment of VPN.

Conventional network infrastructure

First, let's have a look at a typical network structure that can be found in this form or similar forms in many companies:

EN



The corporate network is based on the internal network (LAN) in the headquarters. This LAN is connected to the outside world in three ways:

1 A subsidiary is connected to the LAN, typically using a leased line.

2 PCs dial into the central network via modem or ISDN connections (remote access—RAS).

3 The central LAN has a connection to the Internet so that its users can access the Web, and send and receive e-mail.

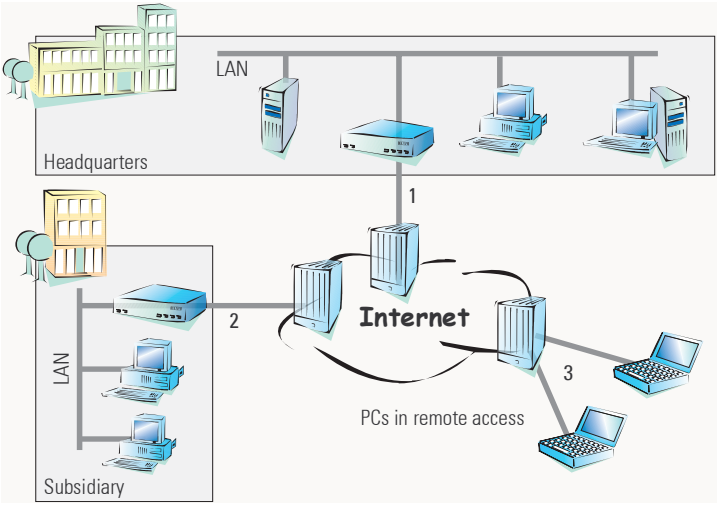
All connections to the outside world are based on dedicated lines, i.e. switched or leased lines. Dedicated lines are very reliable and secure. On the other hand, they involve high costs. In general, the costs for dedicated lines are dependent on the distance. Especially in the case of long-distance connections, keeping an eye out of cost-effective alternatives can be worthwhile.

The appropriate hardware must be available in the headquarters for every type of required connection (analog dial-up, ISDN, leased lines). In addition to the original investment costs, ongoing costs are also incurred for the administration and maintenance of this equipment.

EN

Networking via the Internet

The following structure results when using the Internet instead of direct connections:



All participants have fixed or dial-up connections to the Internet. Expensive dedicated lines are no longer needed.

1 All that is required is the Internet connection of the LAN in the headquarters. Special switching devices or routers for dedicated lines to individual participants are superfluous.

2 The subsidiary also has its own connection to the Internet.

3 The RAS PCs connect to the headquarters LAN via the Internet.

The Internet is available virtually everywhere and typically has low access costs. Significant savings can thus be achieved in relation to switched or dedicated connections, especially over long distances.

The physical connection no longer exists directly between two participants; instead, the participants rely on their connection to the Internet. The access technology used is not relevant in this case: it can be a conventional ISDN line. Broadband technologies such as DSL, cable modems or 2-Mbit leased lines can also be used.

The technologies of the individual participants do not have to be compatible to one another, as would be the case for conventional direct connections. A

single Internet access can be used to establish multiple simultaneous logical connections to a variety of remote stations.

The resulting savings and high flexibility makes the Internet (or any other IP network) an outstanding backbone for a corporate network.

Two technical properties of the IP standard speak against using the Internet as a part of a corporate network, however:

- The necessity of public IP addresses for Internet users
- The lack of data security of unprotected data transfers

1.2.1 Private IP addresses on the Internet?

The IP standard defines two types of IP addresses: public and private. A public IP address is valid worldwide, while a private IP address only applies within a closed LAN.

Public IP addresses must be unique on a worldwide basis. Private IP addresses can occur any number of times worldwide; they must only be unique within their own closed network.

Normally, PCs in a LAN only have private IP addresses, while the router to the Internet also has a public address. Other computers with public IP addresses can only communicate via the Internet with such routers. PCs in the LAN with private addresses can not be addressed from the Internet.

Routing at the IP level with VPN

IP connections must be established between routers with public IP addresses in order to link networks via the Internet. These routers provide the connections between multiple subnetworks. When a computer sends a packet to a private IP address in a remote network segment, the local router forwards the packet to the router of the remote network segment via the Internet.

VPN handles the conversion between private and public IP addresses. Without VPN, computers without public IP addresses would not be able to communicate with one another via the Internet.

1.2.2 Secure communications via the Internet?

The idea of using the Internet for corporate communications has been met with skepticism. The reason for this is that the Internet lies beyond a company's field of influence. Unlike dedicated connections, data on the

Internet travels through the network structures of third parties that are frequently unknown to the company.

In addition, the Internet is based on a simple form of data transfer using unencrypted data packets. Third parties can monitor and perhaps even manipulate the contents of these packets. Anyone can access the Internet. As a result, third parties may gain unauthorized access to the transferred data.

VPN—Security through encryption

VPN was developed as a solution to this security problem. If necessary, it can encrypt the complete data communications between two participants. The packets are then unreadable for third parties. The latest and most secure encryption technologies can be used for VPN. A very high level of security can thus be reached. VPN-protected data traffic via the Internet offers a degree of security that at least corresponds to that of dedicated lines.

Codes usually referred to as “keys” are agreed upon between the participants and used for data encryption. Only the participants in the VPN know these keys. Without a valid key, it is not possible to decrypt the data. They thus remain “private”, inaccessible to unauthorized parties.

Send your data through the tunnel—for security's sake

This also explains the nature of a virtual private network: A fixed, physical connection between the devices of the type required for a direct connection does not exist at any time. With the proper technology, third parties can monitor and even record data traffic. As the packets are encrypted by VPN, the actual content of the packets is inaccessible. Experts compare this state to a tunnel: it's open at either end, but perfectly shielded in between. Secure connections within public IP networks are thus also referred to as “tunnels”.

The goal of modern network structures has thus been achieved: secure connections via low-cost IP networks. It's all possible thanks to tunnels.

EN

1.3 VPN connections in detail

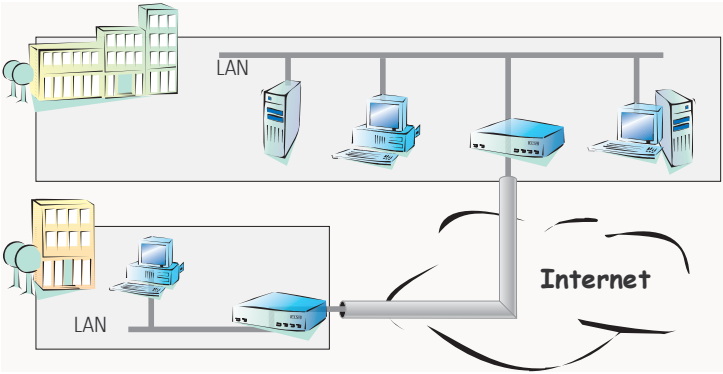
Two types of VPN connections are available:

- VPN connections linking two local networks. This type of connection is also known as a "LAN-LAN coupling".
- The connection of an individual computer with a network, generally via a dial-up connection (RAS).

1.3.1 LAN-LAN coupling

The coupling of two remote networks is known as a LAN-LAN coupling. With such a connection, the devices in one LAN can access those of the remote LAN (assuming they have the necessary access rights).

In practice, LAN-LAN couplings are frequently used between company headquarters and subsidiaries, or for connections to partner companies.



A VPN-enabled router (VPN gateway) is located at either end of the tunnel. The configuration of both VPN gateways must be matched to one another.

The connections are transparent for the remaining devices in the local networks, i.e., they appear to have a direct connection. Only the two gateways must be configured for the VPN connection.

Internet access in parallel

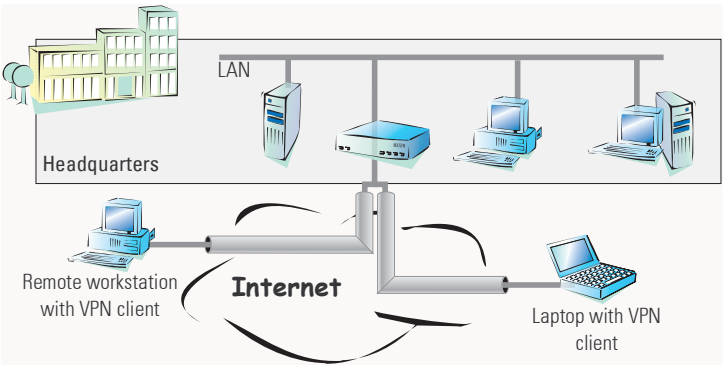
The Internet access for VPN can be used simultaneously for other Internet applications, such as web-browsing or email. For security reasons, the parallel Internet access may be unwanted in some cases. For instance, if a

branch office should be enforced to access the Internet only via a central firewall. For such applications the parallel Internet access can be disabled as well.

1.3.2 Dial-up connections (Remote Access Service)

Individual remote computers (hosts) can access the resources of the LAN via dial-up connections. Practical examples of this are employees working from home or field staff that dial into the company network.

If the dial-up connection of an individual computer to a LAN is to be realized via VPN, that computer first connects to the Internet. A special VPN client software then sets up a tunnel to the VPN gateway of the LAN using this Internet connection.



The VPN gateway of the LAN must support the establishment of VPN tunnels with the VPN client software of the remote PC.

1.4 What is *Dynamic VPN*?

Dynamic VPN is a patent-pending LANCOM Systems technology which permits VPN tunnels to be set up to remote stations that do not have a static, but only a dynamic IP address.

Who needs *Dynamic VPN* and how does it work? We will answer this question in two steps: First, a look at the basics of IP addressing will show the problem of static IP addresses. The second step shows the solution thereof with *Dynamic VPN*.

EN

1.4.1 A look at IP addressing

Every participant on the Internet needs an IP address. Participants even need a special kind of IP address—a public one. The administration of public IP addresses is handled from central locations in the Internet. Each public IP address may only occur once on the entire Internet.

Local IP-based networks do not use public, but private IP addresses. For this reason, a number of address ranges within the entire IP address range have been reserved for private IP addresses.

A computer connected to both a local network and directly to the Internet therefore has two IP addresses: a public one for communication with the rest of the Internet and a private one by which the computer can be reached within the local network.

Static and dynamic IP addresses

Public IP addresses must be applied for and managed, which involves costs. There is also only a limited number of public IP addresses. For this reason, not every Internet user has his or her own fixed (static) IP address.

The alternative to static IP addresses are the so-called dynamic IP addresses. Dynamic IP addresses are assigned to Internet users by their Internet service providers (ISPs) for the duration of the connection when they log in. The ISP therefore uses a random unused address out of his IP address pool. This IP address is only temporarily assigned to the user for the duration of a given connection. When the connection is ended, the IP address is once again free and the ISP can assign it to another user.

Advantages and disadvantages of dynamic IP addresses

This process has a very important advantage for ISPs: they only need relatively small pools of IP addresses. Dynamic IP addresses are also favorable for users: it's not necessary for them to apply for static IP addresses in advance—they can connect to the Internet immediately. It's also not necessary for them to manage IP addresses. This saves trouble and costs. The other side of the coin: A user without a static IP address cannot be addressed directly from the Internet.

This is a major problem when setting up VPNs. If, for example, Computer A would like to communicate with Computer B using a VPN tunnel on the Internet, Computer A needs the remote computer's IP address. If B only has a

dynamic address, A cannot know that address and therefore cannot contact B.

The *Dynamic VPN* offers the answer here.

1.4.2 This is how *Dynamic VPN* works

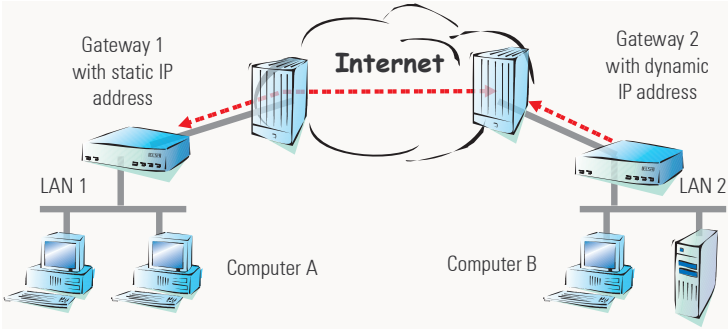
Let's use two examples to explain how *Dynamic VPN* works (designations refer to the IP addressing type of the two VPN gateways):

- dynamic – static
- static – dynamic
- dynamic – dynamic

Dynamic – static

If the user of Computer B in LAN 2 would like to connect to Computer B in LAN 1, Gateway 2 will receive the request and will attempt to set up an VPN tunnel to Gateway 1. Gateway 1 has a static IP address and thus can be addressed directly via the Internet.

The problem is, that the IP address of Gateway 2 is assigned dynamically, and Gateway 2 would have to transmit its current IP address to Gateway 1. Here Dynamic VPN comes into play to accomplish this task.



d Gateway 2 connects to the Internet and is assigned a dynamic IP address.

e Gateway 2 contacts Gateway 1 via its known public IP address. Dyamic VPN enables the identification and transmission of the actual IP address of Gateway 2. Gateway 1 initiates the VPN tunnel then.

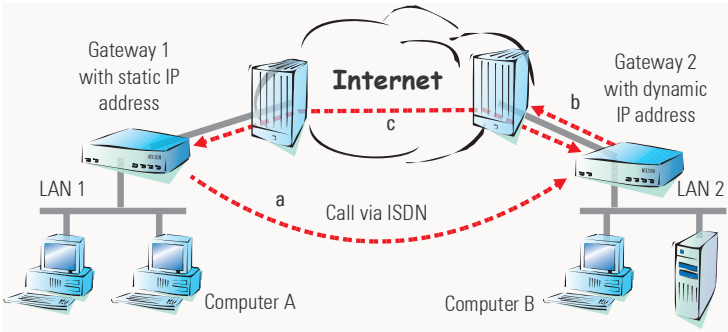
EN

An connection initiated in this direction (from dynamic to static) does not require an ISDN connection at the peers. The site with the dynamic IP address transmits its current IP address in an encrypted packet via the Internet protocol ICMP (or alternatively UDP).

Static – dynamic

If otherwise the user of Computer A in LAN 1 would like to connect to Computer B in LAN 2, Gateway 1 will receive the request and will attempt to set up a VPN tunnel to Gateway 2. Gateway 2 only has a dynamic IP address and thus cannot be addressed directly via the Internet.

With *Dynamic VPN*, the VPN tunnel can be set up nevertheless. The connection is established in three steps:



a Gateway 1 calls Gateway 2 via ISDN. It takes advantage of the ISDN functionality of sending its own subscriber number via the D-channel free of charge. Gateway 2 determines the IP address of Gateway 1 from the preconfigured VPN remote stations using the received subscriber number.

If Gateway 2 does not receive a subscriber number via the D-channel (if that particular ISDN service feature is not available, for example) or an unknown number is transferred, the authentication will be performed via the B-channel. Once the negotiation was successful, Gateway 1 sends its IP address and closes the connection on the B-channel immediately.

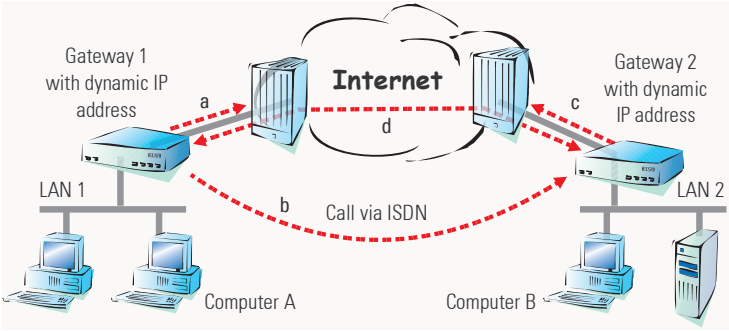
b Now its Gateway 2's turn: It first connects to its ISP and is assigned a dynamic IP address.

c Gateway 2 can now set up the VPN tunnel to Gateway 1. It already knows the static IP address of Gateway 1.

EN

Dynamic – dynamic

With *Dynamic VPN*, VPN tunnels can also be set up between two gateways that both only have dynamic IP addresses. Let's modify the previous example so that in this case Gateway 1 also has a dynamic IP address. Once again, Computer A would like to connect to Computer B:



a Gateway 1 connects to its ISP and is assigned a public, dynamic IP address.

b It then calls Gateway 2 via ISDN to send this dynamic address. Three procedures are used to send the address:

- **As information in the LLC element of the D-channel.** In the D-channel protocol of Euro-ISDN (DSS-1), the so-called LLC (**L**ower **L**ayer **C**ompatibility) element can be used to send additional information to the remote station. This transfer takes place before the B-channel connection is established. Once the address has been sent successfully, the remote station rejects the call. Charges are thus not incurred for a B-channel connection. The IP address is sent nevertheless—for free in this case.

  The LLC element is generally available as a standard feature in Euro-ISDN that does not require registration or activation. It may be disabled by telephone companies or individual exchanges, however. The LLC element is not available in 1TR6, the German national ISDN. The procedure described above thus will not work with 1TR6.

- **As a subaddress via the D-channel.** If it is not possible to send the address via the LLC element, Gateway 1 will attempt to send the address as a so-called subaddress. Like the LLC element, the subaddress is an information element of the D-channel protocol that

EN

permits short items of information to be sent free of charge. In this case, the telephone company must enable the 'subaddressing' feature first; this is generally subject to a charge. As with the LLC element, the call is rejected by the remote station once the IP address has been transferred successfully. The connection thus remains free of charge.

- **Via the B-channel.** If both attempts to send the IP address via the D-channel fail, then a conventional connection via the B-channel must be established to send the IP address. The connection is dropped immediately after the IP address has been sent. This connection is subject to the usual charges.

c Gateway 2 connects to the ISP and receives a dynamic IP address.

d Gateway 2 now sets up the VPN tunnel to Gateway 1.

Dynamic VPN works only between LANCOM that each feature at least one ISDN port that can be used for the ISDN connection.

1.5 An overview of *LANCOM VPN*

This section lists all of the functions and properties of *LANCOM VPN*. This overview will provide a great deal of information for VPN experts. It is very compact, but contains a great deal of complex, specialized terminology. Knowledge of the technical basics of VPN are required to understand this section. Don't worry: it's no problem if you skip this section. The information contained here is not required to set up and use *LANCOM VPN*.

The feature set of LANCOM VPN can vary depending on the particular model and firmware. Information regarding the feature set can be found in the particular device specification. Not all listed features and functions may be present in all LANCOM firmware versions. Please check our Internet site for most recent firmware versions.

- VPN in accordance with IPSec standard
- VPN tunnel via leased lines, switched connections and IP networks
- *Dynamic VPN*: Public IP addresses can be static or dynamic (initiation of a connection towards remote sites with dynamic IP addresses requires ISDN)

- IPSec protocols AH and ESP in transport and tunnel mode
- Hash algorithms:
  - HMAC-MD5-96, Hash length 128 bit
  - HMAC-SHA-1-96, Hash length 160 bit
- Symmetrical encryption methods
  - DES, key length 56 bit
  - Triple-DES, key length 168 bit
  - AES, key length 128 - 256 bit
  - CAST, key length 128 bit
  - Blowfish, key length 128 - 448 bit
- IKE key exchange with Preshared Keys
- Key exchange via Oakley, Diffie-Hellman algorithm with key lengths 768 bit, 1024 bit or 1536 bit, well-known groups 1, 2 and 5
- Key management in accordance with ISAKMP

1.6 What now?

The following chapter will describe the installation of the *LANCOM VPN Option* on a *LANCOM*.

As soon as the *LANCOM VPN Option* is installed on the desired *LANCOM*, go to 'Setting up the VPN connection' on page 25 for the steps needed to establish VPN connections.

EN

2 Installation of the VPN option

This chapter will explain how to install *LANCOM VPN Option* in your *LANCOM*. The installation takes place in six steps:

a Checking the installation requirements

b Online registration

c Activating the VPN option

d Checking the activation

2.1 Installation requirements

Please take a few minutes to check whether all of the requirements for a successful installation have been fulfilled.

2.1.1 Package contents

Please ensure that the package contains the following components:

- *LANCOM* CD with *LANtools*, current firmware and electronic documentation
- Proof of License with license number
- User manual

2.1.2 Access to the device and *LANconfig*

To install the *LANCOM VPN Option*, you need a computer with a Windows operating system (Windows XP, Windows Millennium Edition, Windows 2000, Windows 98, Windows 95, Windows NT 4.0). This computer must have access to the *LANCOM* to be configured. The device's integrated serial configuration port (outband), the LAN (inband) or remote configuration are the available access options.

2.1.3 Latest *LANconfig* version

The most recent LANconfig and LANmonitor versions can be found in the download area of the LANCOM Systems Internet site www.lancom.de. LANCOM Systems recommends to use actual LANtools versions only.

EN

Launching and using LANconfig is described in detail in the documentation of your LANCOM.

2.1.4 Latest firmware version

Most recent firmware versions can be found in the download area of the LANCOM Systems Internet site www.lancom.de. Please select your device from the list and download the appropriate files to your computer. LANCOM Systems recommends to use actual firmware versions only.

Please refer to your LANCOM documentation for details regarding firmware updates.

2.2 Online registration

With the correct firmware version, your *LANCOM* already contains the complete VPN software. It only needs to be activated.

An activation code is required to enable the VPN option in your *LANCOM*.

Please note: *The activation code is not included in the package, but will be sent to you during the online registration.*

A license certificate (Proof of License) containing a license number is included with your *LANCOM VPN Option*. With this license number, you can register at LANCOM Systems to receive your activation code.

A successful online registration cancels the used license number of your LANCOM VPN Option. The activation code that you will receive during registration can only be used on the LANCOM with the specified serial number! Please make sure that you want to install the VPN option on the specified device. It will not be possible to switch to a different device at a later time!

Required registration data

Please have the following information on hand for the online registration:

- Exact designation of the software option
- The license number (from the license certificate)
- Serial number of the *LANCOM* to be activated (on the underside of the device)

- Your customer information (company, name, address, e-mail)

The registration can also be done anonymously, without supplying personal information. The additional information assists us in providing support and service, however. We regard all supplied information to be strictly confidential, of course.

Online input of the registration data

a Launch your web browser and go to the following web page: www.lancom.de/register/routeroption.

b Select your appropriate language.

c Enter the information listed above in the form under 'LANCOM option activation' and follow the additional instructions on the page. After you have entered your information, a page will be displayed containing the activation code for the VPN option of your *LANCOM*, as well as your customer information. If you have supplied your e-mail address, the information and your activation code will also be sent to you via e-mail. The online registration is now complete.

Please store your activation code in a safe place! You may need it again to restore the VPN option, after a repair for example.

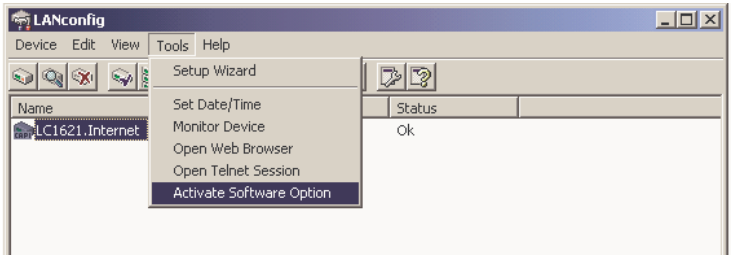
Getting help in case of trouble

If you encounter problems when registering your software option, please contact optionsupport@lancom.de *via email.*

2.3 Activating the VPN option

The VPN option is very easy to activate. In *LANconfig*, select the required *LANCOM* (single click on the entry) and select **Tools / Activate Software Option** menu item:

EN



The 'Activate Software Option' or 'Activate Additional Feature' dialog box will appear:

Activate Software Option
If you have purchased a registration key for an additional feature, enter the key here.
If the key is correct, the new function will be enabled in the device.
Registration key:
This registration applies to one device only. You cannot enter the key for several different devices.
OK
Cancel

Enter the activation code you have received during the online registration described above. Next, the *LANCOM* will reboot.

2.4 Checking the activation

You can verify the successful activation of the *LANCOM VPN Option* by selecting the device in *LANconfig* and selecting the **Device / Properties** menu item. The 'Information' tab of the properties window will display a list of the active software options.

EN

3 Setting up the VPN connection

Once you have installed *LANCOM VPN Option* on the desired *LANCOM*, this chapter will provide you with all of the information needed to set up a VPN connection.

The first section provides general information on using the *LANconfig* Wizard for VPN. The second section provides step-by-step instructions on the VPN configuration, together with a detailed description of all needed input parameters.

Configuration examples for typical VPN connection types can be found in the following chapter.

3.1 The *LANconfig* Wizard for VPN

A separate wizard is not available for VPN. Instead, the existing LAN-LAN Coupling Wizard ('Connect two local area networks') is used. With the activation of *LANCOM VPN*, the VPN queries are added to the LAN-LAN Wizard.

Important requirement: A working Internet access

The LAN-LAN Wizard does not set up an Internet connection. Instead, it assumes and makes use of a functioning Internet access. The Internet access should have been set up with the Set up Internet Access Wizard, before starting to set up the VPN connection with the LAN-LAN Setup Wizard.

The VPN tunnel is being established via the connection defined by the routing table for the IP address of the remote site. That is, in general this would be the standard Internet connection (default route, '255.255.255.255' with netmask '0.0.0.0').

Converting existing connections to VPN connections

To convert existing network couplings to VPN connections, we recommend running the LAN-LAN Wizard completely a second time.

When you are asked for your own device name or that of the remote station, use the same names that the old network coupling uses. Be sure to write them in exactly the same way.

The previous network connection will then be replaced by a VPN-based network connection.

3.2 VPN configuration - step-by-step

Before starting the LAN-LAN Assistant to set up the VPN network coupling, please verify that the following requirements are met:

- The LANCOM VPN option has been enabled on both LANCOM
- If the VPN connection shall use the Internet, ensure that the Internet access on both sites is working properly

3.2.1 Overview of configuration entries

This overview contains all of the questions that the wizard will ask you during the installation. Some questions are not required for certain configurations. We will explain all of the questions nevertheless, but will point out the cases in which they are unnecessary.

A VPN connection always exists between the device to be configured and a known remote station. The configuration is performed on both sides. Care must be taken to ensure that the configuration information provided matches.

The overview also shows the dependencies of the information between the two stations. Noting these dependencies can prevent many incorrect entries.

Entry	Gateway 1		Gateway 2
ISDN connection available?	*yes/no*		*yes/no*
Type of the local IP address	*static/dynamic*		*static/dynamic*
Type of the remote IP address	*static/dynamic*		*static/dynamic*
Name of the local device	*name1*		*name2*
Name of the remote device	*name2*		*name1*
Remote ISDN calling number	*phone number1*		*phone number2*
Remote ISDN caller ID	*ISDN ID1*		*ISDN ID2*
Password for secure transmission of IP address	*password1*		*password1*
Shared Secret for encryption (pre-shared key)	*secret*		*secret*
IP address of remote station	*IP address1*		*IP address2*

Entry	Gateway 1		Gateway 2
IP network address of the remote network	*IP address3*		*IP address4*
Netmask of the remote network	*IP netmask to IP address3*		*IP netmask to IP address4*
Domain name of the remote network	*Domain1*		*Domain2*
Hide local stations in remote network (Extranet VPN)?	*yes =Extranet no = Intranet*		*yes =Extranet no = Intranet*
NetBIOS routing for access to remote network?	*yes/no*		*yes/no*
Name of remote workgroup (NetBIOS only)	*workgroup1*		*workgroup2*

The 'Gateway 1' and 'Gateway 2' columns contain selection options and variables as placeholders for actual configuration information. These placeholders are italicized.

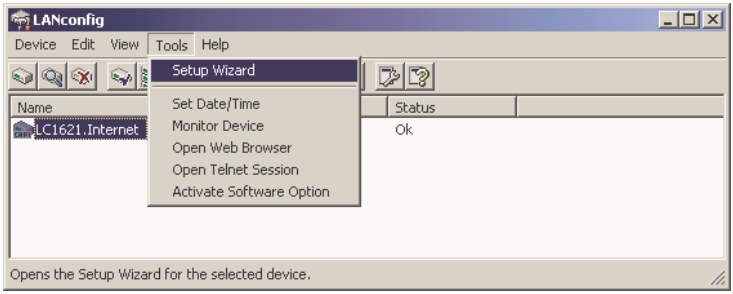
The column between the variables marks required dependencies that must be taken into consideration when making the entries at both gateways. For example, the entries stating whether the VPN connection should be established using a direct connection or via the Internet must be the same for both gateways. Places where the entries must match are marked by arrows (◄►).

This table form will be used for the following step-by-step instructions, was well as for the concrete configuration exsamples of the 3rd section of this paragraph.

3.2.2 Starting the Assitant

To start the wizard, highlight the desired *LANCOM* and select the **Tools / Setup Wizard** menu item:

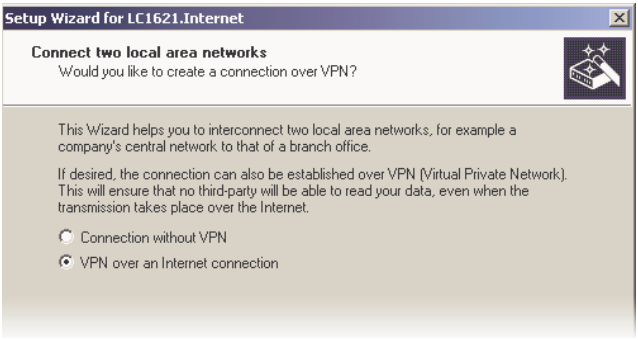
EN



A window then appears with the wizard available for that device. Select the "Connect two local area networks" Setup Wizard.

The use of the wizard is intuitive. All of the parameters needed for the desired connection are queried step by step. **Next** and **Back** can be used to navigate between the windows at any time.

Please specify that the desired network-coupling shall be realized via VPN over an Internet connection:


Setup Wizard for LC1621.Internet
Connect two local area networks
Would you like to create a connection over VPN?
This Wizard helps you to interconnect two local area networks, for example a company's central network to that of a branch office.
If desired, the connection can also be established over VPN (Virtual Private Network). This will ensure that no third-party will be able to read your data, even when the transmission takes place over the Internet.
Connection without VPN
VPN over an Internet connection

All queries are covered in detail in this section. They have been grouped according to topic to improve the overview.

The Assistant automatically skips queries that are unneccessary for the particular scenario. Therefore, it's possible that the Assistant does not query all listed parameters below.

3.2.3 General information on the local device and the remote station

Entry	Gateway 1		Gateway 2
ISDN connection available?	*yes/no*		*yes/no*
Type of the local IP address	*static/dynamic*		*static/dynamic*
Type of the remote IP address	*static/dynamic*		*static/dynamic*
Name of the local device	*name1*		*name2*
Name of the remote station	*name2*		*name1*

The type of IP address must be stated for both sides for VPN connections via the Internet. There are two **types of IP addresses**: static and dynamic. For an explanation of the two IP address types, please see the section 'Send your data through the tunnel—for security's sake' on page 11.

Thank's to *Dynamic VPN*, connections can be enabled not only between gateways with fixed, static IP addresses, but even between gateways with dynamic IP addresses. The active initiation of VPN connections towards remote sites with dynamic IP addresses requires ISDN (see 'What is Dynamic VPN?' on page 13).

In case your device has an ISDN connection, the Assistant asks whether the remote site has ISDN as well.

Then the local IP address type and that of the remote station must be entered. Both entries must match.

If you have not assigned a unique name to your *LANCOM* yet, the Assistants asks to do so now. Providing a **local device name** renames your *LANCOM*. Please ensure that the devices are named differently.

A device name must not consist of numbers only. It must contain at least one non-digit character.

To identify the remote gateway, enter its exact name as **remote device name**.

EN

3.2.4 ISDN connection for *Dynamic VPN*

Entry	Gateway 1		Gateway 2
Remote ISDN calling number	*phone number 1*		*phone number 2*
Remote ISDN caller ID	*ISDN ID1*		*ISDN ID2*

The ISDN parameters are required only when a connection has to be initiated to a gateway with a dynamic IP address.

Therefore, these entries are requested if at least one VPN gateway has an dynamic IP address, and both of the gateways have an ISDN connection.

Enter the calling number of the remote station in the **ISDN calling number** field then. The complete calling number including all necessary area and country codes is required. If your device is connected to the ISDN via a PBX system, a prefix generally will be needed for an external call (usually '0').

The stated **ISDN caller ID** (CLI - **C**alling **L**ine **I**dentfication) is used to identify and authenticate callers. When an *LANCOM* receives a call, it compares the ISDN caller ID entered for the remote station with the actual caller ID transferred via the D-channel. An ISDN caller ID generally consists of an area code and an MSN.

The transmission of the caller ID can be blocked either by your local exchange provider, or by PBX systems. Please ensure that the transmission of the caller ID is enabled at both sites.

3.2.5 Passwords for VPN

Entry	Gateway 1		Gateway 2
Password for secure transmission of the IP address	*Password*	⟷	*Password*
Shared secret for encryption (pre-shared key)	*Shared Secret*	⟷	*Shared Secret*

The **Password for secure transmission of the IP address** is used by *Dynamic VPN* for the exchange of dynamic IP addresses. In case of an ISDN connection, the caller identifies itself with this password, whereas in case of IP address transmission through the Internet (via ICMP or UDP packet), the datagram containing the current IP address is encrypted with this password. The exact same password has to be entered on both sides.

The **Shared Secret** is the central password for security within the VPN tunnel. Strictly speaking, it is not used for encryption, but simply for mutual authentication. The security of the VPN connection is affected decisively by the **Shared Secret**.

Tips for secure passwords

A few number of basic rules must be observed for the handling of passwords:

- **Select a password of suitable length.**
  Each additional character enahances password security. A password should consist of 8 characters at least.
- **Keep your password as secret as possible.**
  Never write a password down. Popular, but completely unsuitable storage options include: notebooks, wallets, and text files in your computer. It sounds trivial, but it can't be repeated often enough: Do not pass on your password. The most secure systems surrender to talkativeness.
- **Only send passwords in a secure manner.**
  A selected password must be reported to the other side. To do this, select the most secure method possible. Avoid: unprotected e-mail, letter, fax. It is better to convey a password personally while alone with the other person. The maximum security is achieved when you personally enter the password at both ends.
- **Select a secure password.**
  Use randomly chosen letter and number sequences. Passwords from common language usage are not secure. Special characters such as '&“?#-*+_:;,!°' also make it more difficult for attackers to guess your password and increase the security of the password.
- **Never use a password twice.**
  If you use the same password for several purposes, you reduce its security effect. If one station is insecure, this automatically jeopardizes the security of all other connections that use the same password.
- **Change the password regularly.**
  Passwords should be changed as frequently as possible. This requires effort, however considerably increases the security of the password.
- **Change the password immediately if you suspect someone else knows it.**
  If an employee with access to a password leaves the company, it is high time to change this password. A password should also always be changed when there is the slightest suspicion of a leak.

EN

3.2.6 The IP address of the remote station

Entry	Gateway 1	Gateway 2
IP address of remote station	*IP address1*	*IP address2*

The **IP address of the remote station** is required to set up the VPN connection for a VPN connection via the Internet to a remote station with a public static address.

3.2.7 TCP/IP Routing settings

Entry	Gateway 1	Gateway 2
IP network address of the remote network	*IP address3*	*IP address4*
Netmask of the remote network	*IP netmask to IP address3*	*IP netmask to IP address4*
Domain name of thre remote network	*Domain1*	*Domain2*
Access to stations in local network permitted?	*yes = Intranet no = Extranet*	*yes = Intranet no = Extranet*

The routing settings are not specific to VPN connections, but are required for all routed LAN-LAN couplings.

VPN network couplings are sensitive to wrong TCP/IP routing information. Please ensure that the routing information to the remote network exactly match the particular situation. Otherwise, the VPN tunnel might not be set up as desired.

For routed network couplings, care has to be taken that both networks are separated logically from each other. Therefore, both networks must have different network addresses and numbers ('10.10.1.x' and '10.10.2.x' for example).

The **IP address of the remote network** is always entered together with the associated **netmask**.

EN

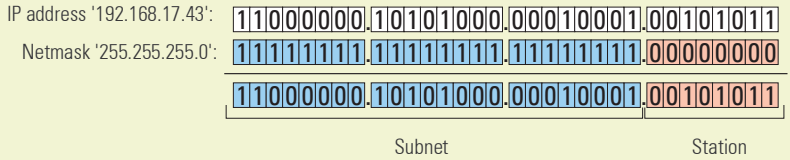
What is a netmask?

An IP address consists of four numbers, each in between 0-255. Technically spoken, these numbers are 4 bytes, consisting of 8 bit each.

The IP address of a network station is defined by the address of the subnet of which the station is a part of, and its address within the subnet. The 32 bit of an IP address can be flexibly assigned to the subnet and the station's address part. This enables different sized subnets. This partitioning is established with the netmask.

The netmask consists of 4 bytes = 32 bits as well. Written in binary format, bits corresponding to a netmask value '1' make up the subnet address part. According to that, digits corresponding to a netmask value '0' make up the stations' addresses.

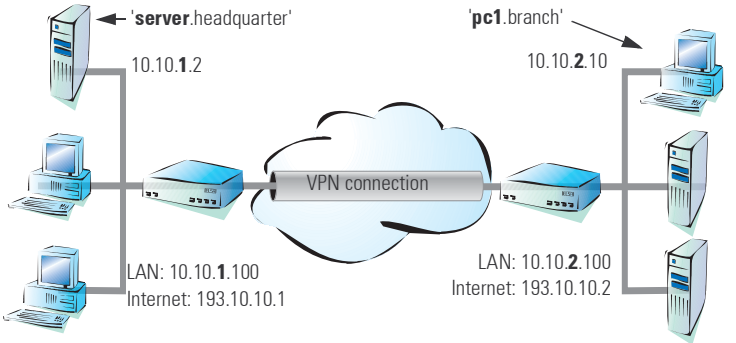
For example, the IP address '192.168.17.43' in conjunction with the netmask '255.255.255.0' addresses the IP station '43' within the subnet '192.168.17.0.



Thanks to DNS (**D**omain **N**ame **S**ystem), the the access to remote PCs in IP networks can be done with names, rather than via IP addresses as well.

For example, a PC with the name 'pc1.branch.company' (IP address 10.10.2.10) can access a server in its entprises headquarters not only by its IP address, but also by its name 'server.headquarters.company'. The only required prerequisite: The **Domain of the remote network** must be entered in the Assistant. In this example, one would have to enter 'branch' as the domain name of the remote network on the headquarters' VPN gateway, and, accordingly, 'headquarters' at the branch office's VPN gateway.

EN



LAN at headquarters: IP: 10.10.**1.0**
Netmask: 255.255.255.0
Domain: '**headquarter**'

LAN at branch office: IP: 10.10.**2.0**
Netmask: 255.255.255.0
Domain: '**branch**'

Please ensure that the DNS servers of the local and remote nework are fully functional. If the remote VPN gateway is not the DNS server for the domain of the remote network as well, then the appropriate DNS server for the remote domain address must be specified in the local VPN gateway. Further information on DNS configuration can be found in the LANCOM reference manual.

Finally, one can decide whether **Access to local stations** is **permitted.**.

In this 'Extranet VPN' operating mode, the IP stations do not expose their IP address to the remote LAN, rather they will be hidden behind the VPN gateway's IP address instead.

Therefore, the stations within the remote LAN cannot access IP stations in the other LAN directly. For example, if a headquarters' LAN in 'Extranet VPN' mode is hidden behind its gateway's address '10.10.2.100', and on of its IP stations (e.g. '10.10.2.13') accesses the IP station '10.10.1.2' of the branch office, then the branch office's IP stations deems to be a accessed by '10.10.2.100'. The true IP address of the accessor ('10.10.2.13') is hidden.

If two LANs shall be coupled in Extranet mode, please ensure to enter the 'outbound' Extranet IP address of the remote site, not its Intranet address. According to the example, this was 10.10.2.100. The appropriate netmask for the Extranet IP address would be 255.255.255.255 then.

3.2.8 NetBIOS routing

Entry	Gateway 1		Gateway 2
NetBIOS routing for access to remote network?	*yes/no*		*yes/no*
Name of remote workgroup (NetBIOS only)	*workgroup1*		*workgroup2*

The information for NetBIOS routing is also not VPN-specific, but is queried at the IP level for all LAN-LAN couplings.

The NetBIOS protocol is used by some network systems for access to shared resources (mostly servers and printers). A common example for the use of NetBIOS: Windows networking.

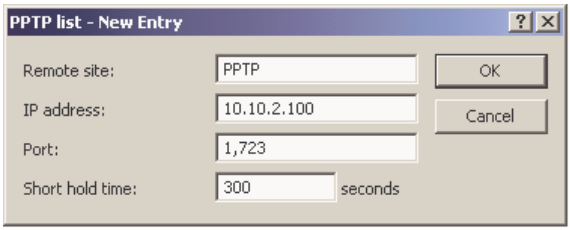
Remote Windows workgroups do not appear in the Windows network neighborhood. Stations in remote Windows networks can be accessed only directly (for example by creating a shortcut to the remote computer on the desktop, or by 'search computer').

3.2.9 IPX Routing

In general, it is not possible to transport IPX packets over a IPSec connection directly. But, instead, it possible to set up a PPTP tunnel inside the IPSec connection of the two LANCOM VPN gateways. The PPTP tunnel is able to transport the IPX packets then.

In *LANconfig*, create a new remote site in the **PPTP list** on the register card **Communication / Protocols**. For convenience, the remote site is named 'PPTP' in the following example. Enter the Intranet IP address of the remote *LANCOM* VPN gateway there and leave the port unchanged. If you enter a short hold time, the PPTP connection is disconnected after this time period automatically

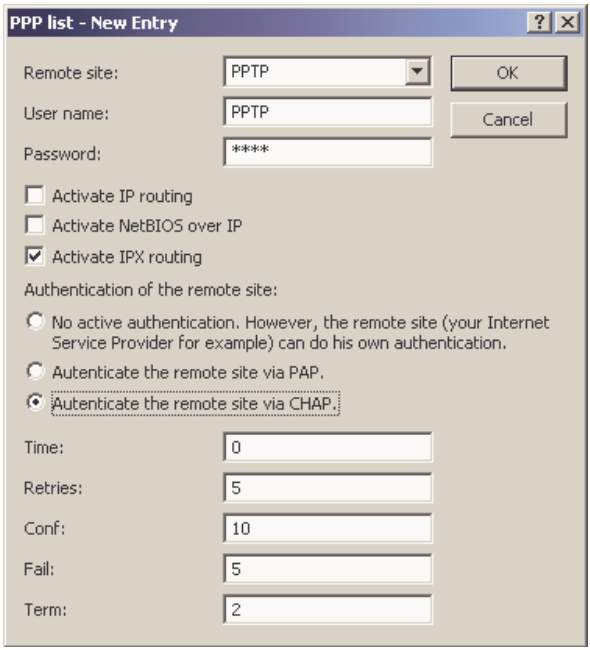
.



EN

Now create a new remote site with the same name in the **PPP list** on the register card **Communication / Protocols** (again, 'PPTP' in this example). The local user name must match the name of the distant remote site. In this example, both has been set to 'PPTP' again. The password must match on both sides as well.

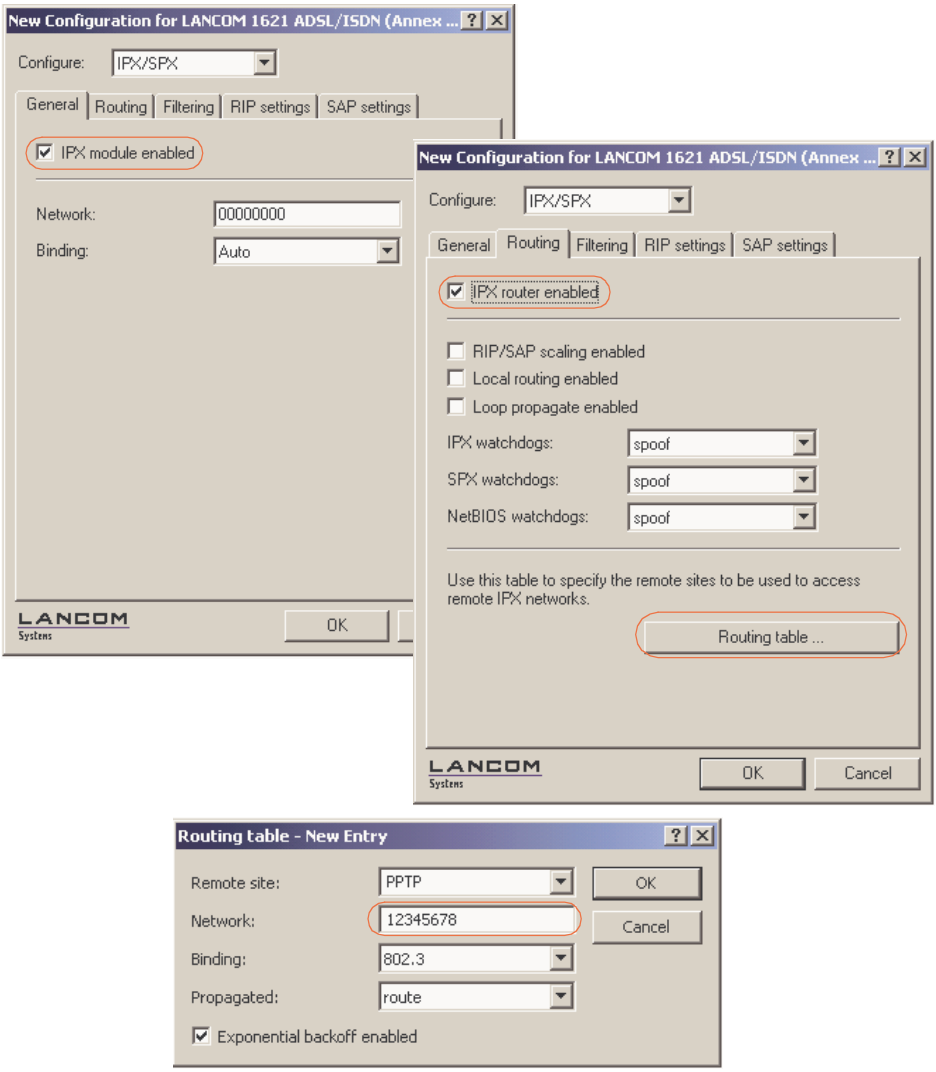
Activate the IPX routing and enable CHAP authentification. All other parameters can be left unchanged to its default values.



The next step is to enable the IPX routing on both sides. Therefore, create a new entry in the Routing table on the IPX/SPX / Routing property page. The network to be entered identically in both of the Routing tables describes the so-called 'IPX transfer network'.

The 'IPX transfer network' - '12345678' in the example figure below - must be different to the local IPX networks described on the register card **General**. *The LANCOM tries to indentify the local IPX network settings itself from the monitored Novell server traffic if one enters '00000000' as the local IPX network, and 'Auto' as Binding there. In case of a remote site without local Novell servers, just enter a unique network number (e.g. '00001111') for the local network then.*

EN


New Configuration for LANCOM 1621 ADSL/ISDN (Annex ...
Configure: IPX/SPX
General Routing Filtering RIP settings SAP settings
IPX module enabled
Network: 00000000
Binding: Auto
LANCOM Systems
OK
New Configuration for LANCOM 1621 ADSL/ISDN (Annex ...
Configure: IPX/SPX
General Routing Filtering RIP settings SAP settings
IPX router enabled
RIP/SAP scaling enabled
Local routing enabled
Loop propagate enabled
IPX watchdogs: spoof
SPX watchdogs: spoof
NetBIOS watchdogs: spoof
Use this table to specify the remote sites to be used to access remote IPX networks.
Routing table ...
LANCOM Systems
OK
Cancel
Routing table - New Entry
Remote site: PPTP
Network: 12345678
Binding: 802.3
Propagated: route
Exponential backoff enabled
OK
Cancel

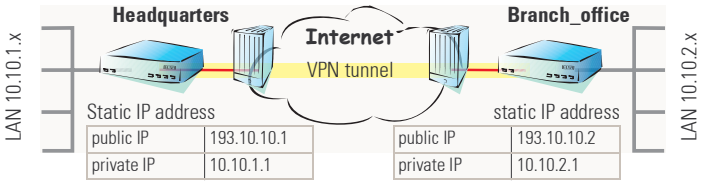
4 Examples of VPN configurations

This section covers the 4 possible types of VPN connections with concrete examples. These 4 different connection types are categorized by the type of IP address of the two VPN gateways:

- static/dynamic
- dynamic/static (the dynamic peer initiates the connection)
- static/dynamic (the static peer initiates the connection)
- dynamic/dynamic

There's a section for each of these types, together with a description of all required configuration information in the familiar table form.

4.1 Static/static

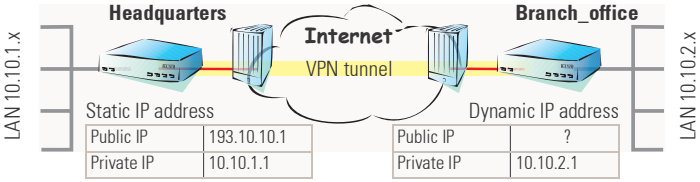


A VPN tunnel via the Internet serves as the connection between the *LANCOM* **Headquarters** and **Branch_office**. Both gateways have static IP addresses. Thus, both can initiate the connection.

Entry	Headquarters		Branch_office
Type of own IP address	static	⇄	static
Typ of remote IP address	static	⇄	static
Name of the local device	Headquarters	⇄	Branch
Name of the remote device	Branch	⇄	Headquarters
Shared Secret für IPSec encryption	*secret*	⟷	*secret*
IP address of the remote device	193.10.10.2		193.10.10.1
IP network address of the remote network	10.10.2.0		10.10.1.0
Netmask of the remote network	255.255.255.0		255.255.255.0

EN

4.2 Dynamic/static



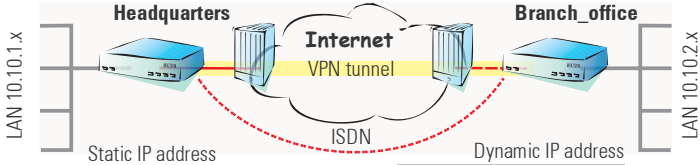
The VPN gateway **Branch_office** initiates a VPN connection to the gateway **Headquarters**. **Branch_office** has a dynamic IP address, which has been chosen and assigned by its Internet Service Provider on dial-in, whereas **Headquarters** has a fixed, static IP address. When the connection is set up, **Branch_office** transmits its actual IP address to **Headquarters**. This is accomplished by an special ICMP packet (alternatively UDP, port 87).

Entry	Headquarters		Branch_office
Typ of local IP address	static	⇄	dynamic
Typ of remote IP address	dynamisch	⇄	statisch
Name of the local device	Headquarters	⇄	Branch_office
Name of the remote device	Branch_office	⇄	Headquarters
Password for secure transmission of dynamic IP address	*confidential*	↔	*confidential*
Shared Secret for IPSec encryption	*secret*	↔	*secret*
IP address of the remote device	–		193.10.10.1
IP-network address of the remote network	10.10.2.0		10.10.1.0
IP netmask of the remote network	255.255.255.0		255.255.255.0

EN

4.3 Static/dynamic

In this case (other than the example above), the peer with the static IP address initiates the VPN connection.



Static IP address

Private IP	10.10.1.1
Public IP	193.10.10.1
ISDN number	(030) 12345
ISDN caller ID	03012345

Dynamic IP address

Private IP	10.10.2.1
Public IP	?
ISDN number	(069) 54321
ISDN caller ID	06954321

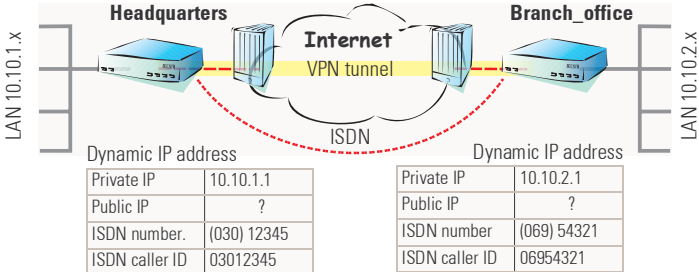
The VPN gateway **Headquarters** initiates the VPN connection to the **Branch_office**. **Headquarters** has a static IP address, **Branch_office** a dynamic one.

The entries for the ISDN connection are needed for the transmission of the actual dynamic IP address solely.

Entry	Headquarters		Branch_office
Type of the local IP address	static	⇄	dynamic
Type of the remote IP address	dynamic	⇄	static
Name of the local device	Headquarters	⇄	Branch_office
Name of the remote device	Branch_offcie	⇄	Headquarters
ISDN-calling number of the remote device	06954321		03012345
ISDN-caller ID of the remote device	06954321		03012345
Password for the secure transmis-sion of the dyn,amic IP address	*confidential*	↔	*confidential*
Shared Secret for the IPSec encryption	*secret*	↔	*secret*
IP-address of the remote site			193.10.10.1
IP-network address of the remote network	10.10.2.0		10.10.1.0
IP netmask of the remote network	255.255.255.0		255.255.255.0

EN

4.4 Dynamic/dynamic



Private IP	10.10.1.1
Public IP	?
ISDN number.	(030) 12345
ISDN caller ID	03012345

Private IP	10.10.2.1
Public IP	?
ISDN number	(069) 54321
ISDN caller ID	06954321

A VPN tunnel via the Internet serves as the connection between the *LANCOM* **Headquarters** and **Branch_office**. Both sides have dynamic IP addresses, and both can initiate the VPN connection.

The entries for the ISDN connection are needed for the transmission of the actual dynamic IP address solely

Entry	Headquarters		Branch_office
Type of local IP address	dynamic	⇄	dynamic
Type of remote IP address	dynamic	⇄	dynamic
Name of the local device	Headquarters	⇄	Branch_office
Name of the remote device	Branch_office	⇄	Headquarters
ISDN-calling number of the remote site	06954321		03012345
ISDN-Anruferkennung Gegenstelle	06954321		03012345
Password for the secure transmission of the dynamic IP address	*confidential*	↔	*confidential*
Shared Secret for the IPSec encryption	*secret*	↔	*secret*
IP network address of the remote network	10.10.2.0		10.10.1.0
IP netmask of the remote network	255.255.255.0		255.255.255.0

EN

5 The technology behind VPN

This chapter explains the technical fundamentals of VPN in general and *LANCOM VPN* in particular. It will provide an overview of the concepts used and the standards on which the technology is based.

This knowledge is not absolutely essential for the use of VPN with *LANCOM*, but it can be helpful. *LANCOM VPN* is designed to let you take advantage of VPN technology without specialized knowledge. VPN connections in particular can be set up without detailed background knowledge.

5.1 How does VPN work?

In practice, a VPN must fulfill a number of requirements:

- Unauthorized third parties must not be able to read the data (encryption)
- It should not be possible to manipulate the data (data integrity)
- Unambiguous identification of the sender of data (authentication)
- Simple key management
- Compatibility to VPN devices from a variety of manufacturers

LANCOM VPN achieves these five major goals by applying the widely used IPSec standard.

5.1.1 IPSec—the foundation of *LANCOM VPN*

The original IP protocol does not contain any provisions for security. Security problems are compounded by the fact that IP packets do not go directly to a specific recipient, but are sent scattershot to all computers on a given network segment. Anyone can help themselves and read the packets. This leaves the door open to the misuse of data.

IP has been developed further for this reason. A secure version is now available: IPSec. *LANCOM VPN* is based on IPSec.

IPSec stands for "**IP Sec**urity Protocol", which was originally the name of a project group within the IETF, the **I**nternet **E**ngineering **T**ask **F**orce. Over the years, this group has developed a framework for a secure IP protocol that is generally referred to as IPSec today.

It is important to note that IPSec itself is not a protocol, but merely the standard for a protocol framework. IPSec actually consists of a variety of proto-

cols and algorithms for encryption, authentication and key management. These standards will be introduced in the following sections.

Security in an IP environment

IPSec has been implemented almost completely within level 3 of the OSI model, i.e. in the network layer. The transfer of data packets using the IP protocol is realized on level 3 of IP networks.

IPSec thus replaces the IP protocol. Under IPSec, the packets have a different internal structure than IP packets. Their external structure remains fully compatible to IP, however. IPSec packets can therefore be transported without problems by existing IP networks. The devices in the network responsible for the transport of the packets cannot distinguish IPSec packets from IP packets on the basis of their exterior structure.

The exceptions in this case are certain firewalls and proxy servers that access the contents of the packets. Problems can arise from the (often function-dependent) incompatibilities of these devices to the existing IP standard. These devices must therefore be adapted to IPSec.

IPSec will be firmly implemented in the next generation of the IP standard (IPv6). For this reason, we can assume that IPSec will remain the most important standard for virtual private networks in the future.

5.1.2 Alternatives to IPSec

IPSec is an open standard. It is not dependent on individual manufacturers and is being developed by the IETF with input from the interested public. The IETF is a nonprofit organization that is open to everyone. The broad acceptance of IPSec is the result of this open structure which unites a variety of technical approaches.

Nevertheless, there are other approaches for the realization of VPNs. We will only mention the two most important of these here. They are not realized at the network level like IPSec, but at the connection and application levels.

Security at the connection level—PPTP, L2F, L2TP

Tunnels can already be set up at the connection level (level 2 of the OSI model). Microsoft and Ascend developed **P**oint-to-**P**oint **T**unneling **P**rotocol (PPTP) early on. Cisco introduced a similar protocol with **L**ayer **2 F**orwarding

(L2F). Both manufacturers agreed on a joint approach which then became the **L**ayer **2 T**unnel **P**rotocol (L2TP) in the IETF.

The objective of the protocols is to ensure security when dialing into networks and replace the PPP and SLIP standards. Their main advantage over IPSec is that any network protocol can be used with such a network connection, especially NetBEUI and IPX.

A major disadvantage of the described protocols is the lack of security at the packet level. What's more, these protocols were designed specifically for dial-up connections. L2TP can also be combined with IPSec to provide enhanced security for dial-up connections.

Security at higher levels—SSL, S/MIME, PGP

Communications can also be secured with encryption at higher levels of the OSI model. Common examples for protocols of this type are SSL (**S**ecure **S**ocket **L**ayer), mainly for Web browser connections, S/MIME (**S**ecure **M**ultipurpose **I**nternet **M**ail **E**xtensions) for e-mail and PGP (**P**retty **G**ood **P**rivacy) for e-mail and files.

In all of the above protocols, an application handles the encryption of the data, for example the Web browser on one end and the HTTP server on the other.

A disadvantage of these protocols in the limitation to specific applications. In addition, a variety of keys is generally required for the different applications. The configuration must be managed on the individual computers and can not be administered conveniently on the gateways only, as is the case with IPSec. Security protocols at the application level tend to be more intelligent as they know the significance of the data being transferred. They are usually much more complex, however.

All of these layer-4 protocols only support end-to-end connections; they are therefore not suitable for coupling entire networks.

On the other hand, these mechanisms do not require the slightest changes to the network devices or access software. And unlike protocols in lower network levels, they are still effective when the data content is already in the computer.

Combinations are possible

All of the alternatives listed above are compatible to IPSec and can therefore be used parallel to it. This permits a further increase of the security level. It

would be possible, for example, to dial into the Internet using an L2TP connection, set up an IPSec tunnel to a Web server and exchange HTTP data between the Web server and the browser in secure SSL mode.

Each additional encryption would reduce the data throughput, however. Users can decide on a case-by-case basis whether the security offered by IPSec alone is sufficient. Higher security will only be required rarely, since the degree of required security can also be set within IPSec.

5.2 The standards behind IPSec

IPSec is based on a variety of protocols for the individual functions. These protocols are based on, and complement one another. The modularity achieved with this concept is an important advantage of IPSec over other standards. IPSec is not restricted to specific protocols but can be supplemented at any time by future developments. The protocols integrated to date also offer such a high degree of flexibility that IPSec can be perfectly adapted to virtually any requirements.

5.2.1 IPSec modules and their tasks

IPSec has to perform a number of tasks. One or more protocols have been defined for each of these tasks.

- Authentication of packets
- Encryption of packets
- Transfer and management of keys

5.2.2 Security associations—numbered tunnels

A logical connection (tunnel) between two IPSec devices is known as an SA (**S**ecurity **A**ssociation). SAs are managed independently by the IPSec device. An SA consists of three values:

- **Security Parameter Index (SPI)**
  ID to distinguish multiple logical connections to the same target device with the same protocols
- **Target IP address**
- **Security protocol used**
  Designates the security protocol used for the connection: AH or ESP

(further information will be provided on these protocols in the following sections).

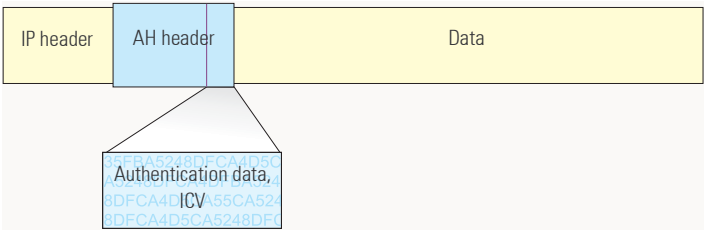
An SA applies only to one communication direction of the connection (simplex). A complete send and receive connection requires two SAs. In addition, an SA only applies for one used protocol. Two separate SAs are also required if AH and ESP are used, i.e. two for each communication direction.

The SAs are managed in an internal database of the IPSec device that also contains the advanced connection parameters. These parameters include the algorithms and keys used, for example.

5.2.3 Authentication—the AH protocol

The AH protocol (**A**uthentication **H**eader) guarantees the integrity and authenticity of the data. Integrity is frequently regarded as a component of authenticity. In the following, we will consider integrity to be a separate problem that is resolved by AH. In addition to integrity and authenticity, AH also provides effective protection against the replay of received packets.

AH adds its own header to IP packets immediately after the original IP header. The most important part of this AH header is a field containing authentication data, often referred to as the **I**ntegrity **C**heck **V**alue (ICV).



The AH process in the sender

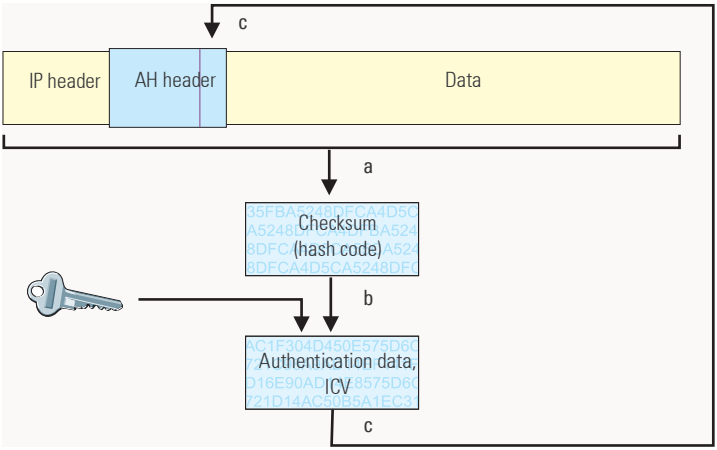
In the sender, the authentication data is generated in 3 steps.

a A checksum is calculated for the complete package using a hash algorithm.

b This checksum is once again sent through a hash algorithm together with a key known to both the sender and the recipient.

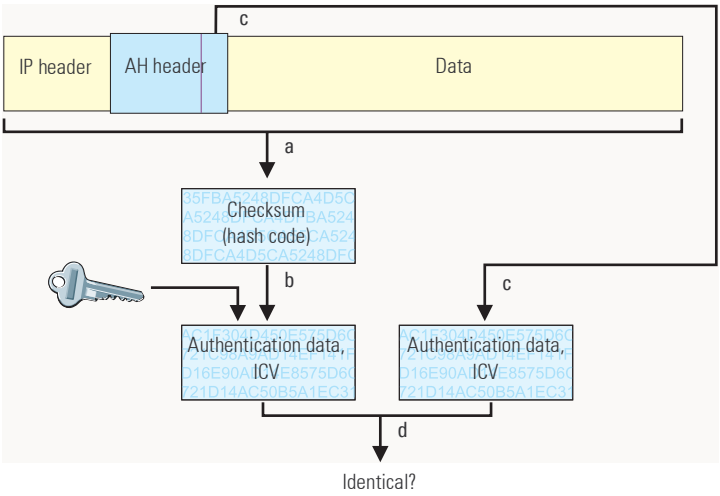
c This results in the required authentication data which is inserted in the AH header.

EN



Checking of integrity and authenticity by the recipient

The AH protocol works in a very similar manner at the recipient's end. The recipient also uses his key to calculate the authentication data for the received packet. The comparison with the sent ICV of the packet determines the integrity and authenticity of the packet.



Determining the checksum for the integrity check

AH adds a checksum to each packet before it is sent to guarantee the integrity of the transferred packets. At the recipients end, AH checks whether the checksum and the contents of the package match. If this is not the case, the packet was either incorrectly transferred or deliberately manipulated. Such packets are discarded immediately and are not forwarded to higher protocol levels.

A variety of so-called hash algorithms are available to determine the checksum. Hash algorithms are distinguished by the fact that their results (the hash code) are a unique fingerprint of the original data. Conversely, the original data cannot be determined on the basis of the hash code.

LANCOM VPN supports the two most common hash algorithms: MD5 and SHA-1. Both methods work without keys, i.e. on the basis of fixed algorithms. Keys do not play a role until a later step of AH: the final generation of the authentication data. The integrity checksum is only a necessary intermediate result on the way there.

Generation of the authentication data

In the second step, AH generates a new hash code using the checksum and a key—the final authentication data. A variety of standards are available under IPSec for this process as well. *LANCOM VPN* supports HMAC (**H**ash-based **M**essage **A**uthentication **C**ode). The hash functions MD5 and SHA-1 are available as hash algorithms. The HMAC versions are accordingly known as HMAC-MD5-96 and HMAC-SHA-1-96.

This clarifies why AH leaves the packet itself unencrypted. Only the checksum of the packet and the local key are added to the packet together with the ICV, the authentication data, in encrypted form as a verification criterion.

Replay protection—protection against replayed packets

In addition to the ICV, AH assigns a unique sequence number to each packet. The recipient can thus recognize which packets were intercepted by a third party and resent. Attacks of this type are known as "packet replay".

The sender adds such a sequence number to each packet by default before sending it on its way. If the recipient decides that replay protection is not required, the sender stops numbering the packets.

EN

5.2.4 Encryption of the packets—the ESP protocol

The ESP protocol (**E**ncapsulating **S**ecurity **P**ayload) encrypts the packets as protection against unauthorized access. This was once the only function of ESP, but in the course of the further development of the protocol it was expanded with options for the protection of integrity and verification of authenticity. In addition, ESP also features effective protection against replayed packets. ESP thus offers all of the functions of AH—in some cases, however, the use of AH parallel to ESP is advisable.

How ESP works

The structure of ESP is more complex than that of AH. ESP also inserts a header behind the IP header as well its own trailer and a block of ESP authentication data.

Transport and tunnel mode

Like AH, ESP can be used in two modes: transport and tunnel mode.

In transport mode, the IP header of the original packet is left unchanged and the ESP header, encrypted data and both trailers are inserted.

The IP header contains the unchanged IP address. Transport mode can therefore only be used between two end points, for the remote configuration of a router, for example. It cannot be used for the coupling of networks via the Internet—this would require a new IP header with the public IP address of the recipient. In such cases, ESP can be used in tunnel mode.

In tunnel mode, the entire packet including the original IP header is encrypted and authenticated and the ESP header and trailers are added at the entrance of the tunnel. A new IP header is added to this new packet, this time with the public IP address of the recipient at the end of the tunnel.

Encryption algorithms

As a higher-level protocol, IPSec does not require specific encryption algorithms. The manufacturers of IPSec products are thus free in their choice of the processes used. The following standards are common::

- **AES - Advanced Encryption Standard**
  AES is the official encryption standard for use by US authorities, and therefore one of the most important standards worldwide. In the year 2001, the US **N**ational **I**nstitute of **S**tandards and **S**ecurity (NIST) chose the AES algorithm (also known under its former name Rijndael) as the winner of a worldwide contest between different encryption algorithms. AES is a symmetric key algorithm with variable block and encryption lengths. It has been developed by the Belgian scientists Joan Daemen und Vincent Rijmen, and features outstanding security, flexibility and efficiency.
- **DES - Data Encryption Standard**
  DES was developed by IBM for the NSA (National Security Agency) in the early 1970s and was the worldwide security standard for years. The key length of this symmetrical process is 56 bits. Today, it is considered to be insecure due to its short key length and should therefore not be used if possible.
- **Triple-DES** (also 3-DES)
  A further development of DES. The conventional DES algorithm is applied three times consecutively. Two or three different keys, each with a length of 56 bits are used. Triple-DES uses two different keys for the three DES runs. The key for the first run is reused for the third DES run. The result is a nominal key lenght of 168 bit, with an effective key length of 112 bits.

  Triple-DES combines the sophisticated DES technology with a sufficiently long key and is therefore considered to be highly secure. Triple-DES is slower than other processes, however.
- **Blowfish**
  This development by the renowned cryptographer Bruce Schneier is a symmetrical encryption process. Blowfish achieves outstanding data throughput on multifunction processors. The process is reputed to be extremely efficient and secure. Blowfish is selected by default with a key length of 128 bits for *LANCOM VPN* by the LAN-LAN Wizard.
- **CAST** (named after its authors, **C**arlisle **A**dams and **S**tafford **T**avares)
  is a symmetrical process with a key length of 128 bits. CAST permits the modification of parts of the algorithm at runtime.

The encryption settings can be modified in the expert configuration under LANconfig. Modifications of this sort are generally only required when setting up VPN connections between devices from different manufacturers.

EN

5.2.5 Key management—IKE

The **I**nternet **K**ey **E**xchange Protocol (IKE) permits the integration of subprotocols for managing the SAs and for key administration.

Within IKE, two subprotocols are used in *LANCOM VPN*: Oakley for the authentication of partners and key administration, and ISAKMP for managing the SAs.

Setting up the SAs with ISAKMP/Oakley

Each setup of an SA is performed in several steps (in the case of dynamic Internet connections, these steps are performed after the public IP address has been transferred):

a The initiator sends a plain-text message to the remote station via ISAKMP with the request to set up an SA and with proposals for the security parameters of the SA.

b The remote station replies with the acceptance of a proposal.

c Both devices now generate key pairs, each consisting of a public and private key, for Diffie-Hellman encryption.

d In two further messages, the devices exchange their public keys for Diffie-Hellman.

e The further communication is encrypted with Diffie-Hellman. The initiator sends a hash value of his Shared Secret. The remote station verifies the hash value and replies with the hash value of its own Shared Secret. An encrypted connection in which both partners have authenticated themselves exists as of this point. Phase 1 of the SA setup is thus completed.

f In Phase 2, the session keys for the authentication and symmetrical encryption of the actual data transfer are generated at random and transferred.

Symmetrical processes are used for the encryption of the actual data transfer. Asymmetrical processes (also known as public-key encryption) are more secure as they do not require the exchange of secret keys. However, they require considerable processing resources and are thus significantly slower than symmetrical processes. In practice, public-key encryption is generally only used for the exchange of key material. The actual data encryption is then performed using the fast symmetrical process.

The regular exchange of new keys

ISAKMP ensures that new key material is regularly exchanged between the two devices during the SA. This takes place automatically and can be checked using the 'Lifetime' setting in the advanced configuration of *LANconfig*.

6 Index

Numerics
3-DES 19, 51
A
Activating the VPN option 22, 23
AES 19, 51
AH 19, 47
B
Blowfish 19, 51
C
CAST 19, 51
D
DES 51
DES, 19
Device name 29
DNS server 34
Domain 33
Dynamic VPN
    dynamic - dynamic 17, 42
    dynamic - static 15, 40
    Examples 39
    Overview 15
    static - dynamic 16
    static/dynamic 41
E
ESP 19, 50
Extranet VPN 34
F
Firmware 3, 22
Frequently asked questions (FAQs) 3
H
Hash algorithms 19, 49

EN

I
ICMP 16, 40
IKE 19, 52
Information symbols 4
Installation 21
Internet access 25
IP addresses
    dynamic 14
    static 14
IPSec 43
IPv6 44
ISAKMP 19
ISDN
    B-channel 18
    caller ID (CLI) 30
    D-channel 17
    Euro-ISDN (DSS-1) 17
    LLC 17
K
KnowledgeBase 3
L
L2F 44
L2TP 44
N
NetBIOS 35
Netmask 33
O
Online registration 23
P
Package contents 21
Passwords
    Secure transmission of the IP address 30
    Shared Secret 31
    Tips for secure passwords 31

PPTP 35, 44
Preshared Key 19
    Shared Secret 31
Proof of License 21
Public key 52
R
Registration 22, 23
S
Support 3
T
Text formatting 4
Triple-DES 51

EN